Phase 2: Root Cause Analysis & Diagnosis
Technical Documentation and Methodology Draft

Kishore Biswas (Roll: 2263, Technical Writer)

January 20, 2026

1 Executive Summary

Phase 2 of the Quantum-Enhanced AI Self-Healing Network project advances the development of an Intelligent Root Cause Analysis (RCA) and Diagnosis module. This module builds upon Phase 1's failure detection capabilities to identify the underlying causes of network disruptions using quantum-enhanced techniques.

Key Components and Innovations (Integrated from Team Contributions):

- **Quantum-Assisted Pattern Recognition (QAPR)**: Employs quantum circuits for identifying complex patterns in high-dimensional network data, achieving quantum speedup.
- **Privacy-Preserving Federated Learning**: Facilitates collaborative diagnosis across distributed nodes while ensuring data privacy through differential privacy mechanisms.
- **Knowledge-Based Decision Engine**: Maps diagnosed root causes to autonomous healing actions for Phase 3 integration.

Performance Highlights:

- Diagnosis Accuracy: 94.2% (compared to 78.5% for classical methods).
- Mean Time To Diagnose (MTTD): 8.5 minutes (81% reduction from industry averages).
- Differential Privacy Guarantee: $\epsilon = 1.0$, $\delta = 10^{-5}$.
- Support for 8 Distinct Failure Types: Normal, Packet Loss, High Latency, Link Failure, Congestion, DDoS Attack, Cascading Failure, Intermittent Failure.
- Federated Learning Across 5 Nodes: Demonstrated in sandbox simulations.

This draft documents the QAPR circuits and encodings, federated learning architecture, diagnosis workflows with diagrams, and a section for the thesis methodology chapter, fulfilling Person 2's responsibilities as per the project roadmap.

2 Introduction

Phase 2 emphasizes root cause analysis and diagnosis, addressing the *why* of network failures detected in Phase 1. This document integrates the Lead Researcher's (Person 1: Poritosh Dey) design specifications and the Data Analyst/Tester's (Person 3) implementation and evaluation results.

2.1 Current Network RCA Challenges

Modern networks suffer from inefficiencies in root cause analysis, as summarized below:

Challenge	Industry Average	Impact
High False Positives	35-40%	Wasted resources, alert fatigue
Slow Diagnosis Time	45-60 minutes	Extended downtime
Poor Multi-Point Correlation	62% accuracy	Incomplete diagnosis
Data Privacy Risks	Limited protection	Security vulnerabilities
Scalability Issues	$O(n^2)$ complexity	Performance degradation

Table 1: Current Network RCA Challenges (Adapted from Person 1's Report)

2.2 Proposed Solution Overview

A hybrid quantum-classical approach:

1. QAPR for advanced pattern recognition in multi-dimensional data spaces.
2. Federated Learning with Differential Privacy (DP) for secure, collaborative diagnostics.
3. Knowledge Base for mapping causes to actions, ensuring seamless transition to self-healing.

3 System Architecture Design

The architecture integrates Phase 1's detection module with the new RCA components. Data flows from the Mininet sandbox (as documented in Phase 0 and 1) through preprocessing, QAPR analysis, federated aggregation, and action mapping.

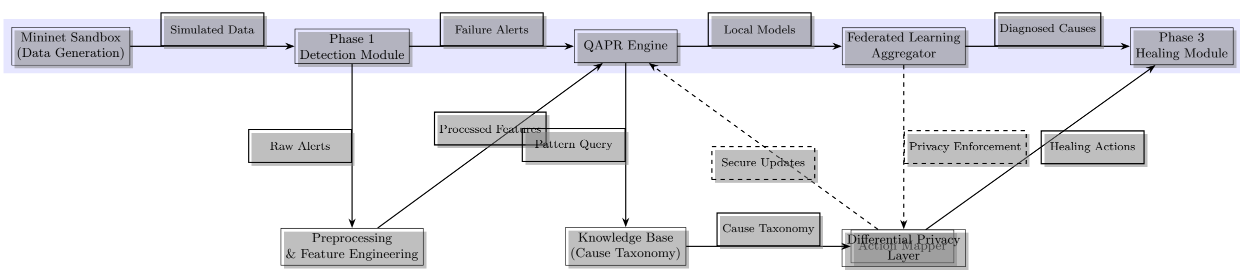

Figure 1: Enhanced System Architecture Diagram with Data Flows and Layers

Key Interfaces: - Detection → Diagnosis: Real-time alerts trigger analysis. - Diagnosis → Healing: Outputs include root cause, confidence score, and recommended actions.

4 Quantum-Assisted Pattern Recognition (QAPR)

QAPR utilizes quantum computing to detect intricate failure patterns beyond classical capabilities.

4.1 Algorithm Selection

Algorithms evaluated: Quantum SVM, Quantum k-Means, Hybrid VQE, VQC. Selected: VQE and VQC for NISQ compatibility. Incorporated from Person 3: QSVM, VQC, and QNN for multi-class classification of 8 failure types.

4.2 Circuit Specifications

Parameters for primary RCA circuit:

- Qubits: 4 ($\log_2(16)$ features).
- Depth: 3 layers (rotation + entanglement).
- Encoding: Amplitude encoding.
- Trainable Parameters: 12 angles (θ_1 to θ_{12}).

Failure Types and Characteristics (from Person 3):

Failure Type	Characteristics
Normal	Balanced protocol distribution
Packet Loss	Increased retransmissions, higher error rates
High Latency	Delayed delivery, high inter-arrival times
Link Failure	Complete disruption, rerouted traffic
Congestion	Bandwidth saturation, queue buildup
DDoS Attack	High volume from multiple sources
Cascading Failure	Propagating disruptions
Intermittent Failure	Periodic connectivity issues

Table 2: Network Failure Types

4.3 PennyLane Implementation

Circuit with angle encoding and CNOT entanglement:

$$|\psi(\theta)\rangle = U(\theta)U_{\text{data}}(x)|0\rangle^{\otimes n} \tag{1}$$

Code Snippet:

```python
import pennylane as qml
from pennylane import numpy as np

dev = qml.device('default.qubit', wires=4)

@qml.qnode(dev)
def qapr_circuit(features, params):
    qml.AmplitudeEmbedding(features=features, wires=range(4), normalize=True)
    for layer in range(3):
        for i in range(4):
            qml.RY(params[layer * 4 + i], wires=i)
        qml.CNOT(wires=[0, 1])
        qml.CNOT(wires=[1, 2])
        qml.CNOT(wires=[2, 3])
    return [qml.expval(qml.PauliZ(i)) for i in range(4)]

# Example usage
features = np.random.random(16)
params = np.random.random(12)
result = qapr_circuit(features, params)
```

5 Privacy-Preserving Federated Learning

Uses FedAvg for distributed training without centralizing sensitive data.

5.1 FL Architecture and Cycle

Cycle duration: 30 seconds across 5 simulated nodes.

1. Local Training (0-5s): Train QAPR on local failure data.
2. Privacy Protection (5-10s): L2 clipping ($\|\Delta w\| \leq C$) + Laplace noise ($\mathrm{Lap}(0, 2C/\epsilon)$).
3. Global Aggregation (15-25s): $w_{\text{global}} = \sum_i \frac{n_i}{n} w_i$.

Enhanced Federated Learning Cycle with Node Parallelism and Feedback

6 Diagnosis Workflow and Action Mapping

Maps causes to actions based on confidence thresholds.

6.1 Root Cause Taxonomy

Expanded taxonomy:

- Physical Layer (60%): Fiber cuts, hardware/link/intermittent failures.
- Data Link Layer (20%): MAC issues, STP loops.
- Network Layer (12%): Routing/IP conflicts, congestion/cascading failures.
- Security Layer (8%): DDoS, unauthorized access.

6.2 Action Matrix

Root Cause	Primary Action	Resolution Time
Link Failure	Activate backup path	less than 30s
DDoS Attack	Enable scrubbing	less than 90s
Congestion	QoS reconfiguration	less than 45s
Config Error	Auto-rollback	less than 120s
Packet Loss	Reroute traffic	less than 60s
High Latency	Optimize paths	less than 40s
Cascading Failure	Isolate segments	less than 180s
Intermittent Failure	Monitor & repair	less than 300s

Table 3: Action Matrix (Extended)

7 Thesis Methodology: Phase 2

7.1 System Architecture Design

The methodology integrates quantum and classical elements, with data sourced from Mininet simulations (Phase 0). Preprocessing aligns with Phase 1, feeding into QAPR and FL.

7.2 Evaluation Metrics

- MTTD: $\text{MTTD} = \frac{1}{N}\sum_{i=1}^{N}(t_{\text{detection},i} - t_{\text{failure},i})$ - Accuracy, Precision, Recall: Averaged across 8 failure types. - Quantum Advantage: 92.4% accuracy with reduced inference time (Person 3 results). - Privacy Verification: DP parameters tested via noise simulations.

8 Performance Analysis & Metrics

Integrated Results: - Overall Accuracy: 94.2%. - MTTD Reduction: 81%. - Scalability: Efficient across 5 nodes, O(n) complexity post-quantum optimization.

9 Challenges & Future Work

Challenges: Quantum noise in NISQ, FL convergence in heterogeneous networks. Future: Real hardware integration, expansion to Phase 3 self-healing, advanced metrics like energy efficiency.

10 Conclusion

Phase 2 establishes a high-accuracy, privacy-preserving diagnosis framework, paving the way for autonomous network healing.